What is domain trust?

Domain trust is a concept used to establish trust between domains. If there is trust between two domains users can access resources in the other domain.

`Domain forest` is a group of domains that trust each other. Forests maybe also have trust between them.

Types of trust

- Parent/Child

Part of the same forest. Retains an implicit two-way transitive trust.

I think this might be stuff like child: test.mydomain.local, and parent mydomain.local.

- Crosslink

Transitive trust.

If Domain A trusts Domain B, and Domain B trust domain C, then Domain A trusts Domain C. So you can have trust-chains.

Directional trust

You can have One way trust and bidirectional trust. A bidirectional trust is simply two one-way trusts.

If A is trusted by B. That means that A can access resources in B. Think of it like this: If A is trusted by B, then B will let A into his house.

Attack Strategy

As always the first part of an attack is enumeration. We need to know the following: 1. Which domains have trusts with each other Essentially create a map of trusts between domains.

2. Enumerate any user/group/computer (security principals) that in one domain that has access to resources in another domain. For example, member in local Admin group. What we want to do is look for some kind of bridge between the two domains. That is usually the case, because a trust relationship is usually implemented because resources need to be shared over the domain bounderies. It might be possible with kerberoasting over boundries.
3. Exploit the identified targets

Map the domain trusts

This can be done using three techniques: Win32 API Calls, various .NET methods, and LDAP queries.

With PowerShell this can be done with the following code:

```
 ([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).GetAllTrustRelationships()
([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelationships()
```

The functionality is also included in PowerView, and can be run like this:

```
 Get-DomainTrust
Get-ForestTrust
```